Cybersecurity Incident Response Flowchart

Cybersecurity incident response is a critical process designed to identify, contain, and mitigate security threats. By following a structured response plan, organizations can minimize damage and prevent future attacks. This flowchart outlines the essential steps in handling security incidents.

Step-by-Step Process:

- Detect Security Threat

A potential security breach is identified through monitoring tools, user reports, or automated alerts.

- Analyze Threat

The IT security team investigates the incident, determining its severity and potential impact on systems.

- Critical Threat?

If the threat is classified as critical, immediate containment measures are initiated to prevent further damage.

- Apply Mitigation

For non-critical threats, mitigation strategies such as firewall updates, user access restrictions, or security patches are applied.

- Deploy Security Patch

If vulnerabilities are detected, a security patch is implemented to close the security gap.

- Monitor System

After applying fixes, the system is continuously monitored for any additional threats or unusual activities.

- Incident Resolved

Once the security team verifies that all risks have been mitigated, the incident is officially closed.